IMPLEMENTATION GUIDE

Essential Eight for Small Business

Start Here

Prepared for: Small business IT administrators

Prepared by: Simple Cyber Security | SimpleCyberSecurity.com.au

Date: 17 August 2026 | Version: 1.0

Introduction

The Essential Eight is straightforward to understand in principle, but often much harder to implement well in a real environment. This series is designed to close that gap.

Rather than simply restating the requirements, the Simple Cyber Security Essential Eight implementation series focuses on what those requirements look like in practice: what needs to be changed, and why. Of course, making changes without verification is a guessing game, so the before-and-after checks are also covered.

This document is the first in this implementation series.

Disclaimer

ASD announced in June 2026 that the Essential Eight would evolve into a broader Essentials series, beginning with Essentials for enterprise IT. At the time this guide was prepared, the Essential Eight guidance and November 2023 maturity model remained published. Reasonable efforts have been made to keep this material accurate and current; however, cyber security guidance, technologies, and vendor platforms change over time, and SCS cannot guarantee that all content will remain current or applicable in every environment.

The Essential Eight is developed and maintained by the Australian Signals Directorate and Australian Cyber Security Centre. This guide is an independent SCS resource intended to support practical implementation of that model. SCS does not claim ownership of the Essential 8 or endorsement by ASD or ACSC, and references the authoritative source material where appropriate. Following this guide does not in itself guarantee compliance, a particular maturity level, or protection from cyber security incidents.

KEY POINTS

- This guide is not an official ASD or ACSC course and does not replace official guidance.
- Completing a process does not automatically mean the entire organisation has achieved a maturity level.
- The Essential Eight does not address every cyber threat or every security responsibility of a business.
- The reader remains responsible for testing changes and deciding whether they are appropriate for the business.
- This guide is provided as general implementation support for small businesses. Consider the guidance in the context of your own environment and modify the processes where appropriate.

Contents

Start Here

This is the first guide in the Simple Cyber Security Essential Eight implementation series. It provides the foundation for the guides that follow, including how the framework is structured, why the Essential Eight is a practical goal for small businesses, the assumptions used throughout the examples, and some considerations before making changes.

The series was created to make the Essential Eight easier to move from guidance into practice. For smaller organisations with limited IT resources, security guidance can quickly become difficult to apply when it assumes dedicated security teams, specialised tools, or significant time and budget. The Essential Eight provides a more focused set of strategies that can still deliver meaningful security improvement and, with the right guidance, can be achievable in a small business environment.

This guide is intended primarily for small businesses and smaller IT environments where there may be no dedicated cyber security team. In many cases, the person using it may already be responsible for the organisation's devices, accounts, applications, cloud services and day-to-day IT support. The guidance is therefore written with the assumption that implementation needs to be practical, understandable, and manageable with limited resources.

The goal of the series is to turn the requirements into practical processes: understand what needs to be done, make the change safely, confirm that it is working as you go, and leave behind something that can continue to be maintained.

Frameworks

Cyber security can become difficult to approach when there is no clear structure for deciding what to protect, what to prioritise, or what good security should look like. Frameworks help solve that problem by providing an organised way to turn broad security goals into a set of defined practices or outcomes.

A framework is a general structure that provides a foundation on which to build. Like the frame of a house, it creates shape and direction, but it is not the finished result.

In the context of the Essential Eight, the framework provides a way to focus effort on a limited number of high-value security controls rather than trying to design an entire cyber security program from scratch.

Why frameworks are useful

- They provide clear and consistent direction.
- They give you a starting point developed from established experience.
- They provide common language, control objectives and examples to follow.

Why the Essential Eight?

Some cyber security frameworks are broad and comprehensive, but implementing them properly can require significant time, specialist expertise and financial investment. For a small business with limited IT resources, the effort needed to interpret the framework, decide what applies, design appropriate controls and maintain them can quickly become impractical.

The challenge is not that these frameworks are ineffective, but that their scale may not suit a smaller organisation. For small businesses, practicality matters: the security objective needs to be realistic within available staff, expertise and budget, clear enough to act on, and achievable enough that the organisation can implement and maintain it over time.

The Essential Eight fits this need by narrowing the focus to eight complementary mitigation strategies, supported by a maturity model that defines what implementation looks like at different levels. This gives a small business a clear and manageable security target: a finite set of strategies with defined outcomes, rather than a broad framework that requires the organisation to determine its own priorities and approach from the outset.

In practical terms, the Essential Eight focuses on eight specific areas of security that together form the scope of the framework. The table below outlines each strategy and the role it plays in reducing cyber security risk.

Strategy	Practical Outcome
Application Control	Only approved applications and code are allowed to run
Patch Applications	Known application vulnerabilities are remediated before they can be exploited
Restrict MS Office Macros	Macros are limited to trusted sources
User Application Hardening	Common risky applications are configured to reduce risk
Restrict Administrative Privileges	Administrative least privilege is implemented and only used when necessary
Patch Operating Systems	Known OS vulnerabilities are remediated before they can be exploited
Multi-Factor Authentication	Risk associated with standalone passwords is reduced
Regular Backups	Reliable backups are available to support recovery

Table 1 - The Essential 8 Strategies

Understanding Maturity levels

The Essential Eight defines four maturity levels, from Maturity Level Zero to Maturity Level Three. With the exception of Level Zero, the levels are based on increasingly capable tradecraft and more deliberate targeting by malicious actors.

Maturity Level One focuses on common, widely available attack techniques and malicious actors looking for opportunities rather than investing significant effort in a particular target. Levels Two and Three progressively address attackers with greater capability, persistence and willingness to tailor their approach to the organisation.

For this series, Maturity Level One is the objective. ASD identifies it as generally suitable for small to medium enterprises[1], and it provides a practical level of protection against the common and opportunistic attacks that small businesses are likely to face. Importantly, it remains a meaningful security target while keeping the implementation, cost and ongoing management within a scope that is more achievable for a small business.

Maturity Level	Security State	Indicative Suitability
Zero	Generally, the business is vulnerable to common vulnerabilities and opportunistic attacks	Not a target state
One	Common weaknesses and opportunistic attacks are less likely to succeed, but targeted attacks may still compromise the organisation.	Small Organisations
Two	Threat actors who target the enterprise will need to invest time and effort to compromise the business, and any compromise is likely to be delayed	Larger Organisations
Three	Threat actors would need to invest significant time and cost to compromise the organisation.	Critical Infrastructure / High-threat environments.

Table 2 - The Essential 8 Maturity Levels

[1] Australian Signals Directorate, Essential Eight Maturity Model FAQ

Test Lab

Throughout this series, a test lab is used to demonstrate each implementation process and show the control working in practice. Where possible, this includes a before-and-after comparison so you can see the behaviour before the control is applied, make the change, and then confirm the expected outcome afterwards.

The lab represents a simple on-premises small business environment, consisting of a domain controller running Windows Server 2022, a web server running Windows Server 2019, and two endpoints running Windows 11 Pro.

The lab does not represent every environment, but the principles and processes can be applied to similar environments. Controls will be configured using approaches that can scale to additional endpoints, servers and, where appropriate, hybrid environments, although some implementation details will differ.

Organisations without an Active Directory domain may need to perform some tasks differently or more manually, and domain-specific configuration steps may not apply. The important part is understanding the intent of each mitigation strategy and applying that intent appropriately to your own environment.

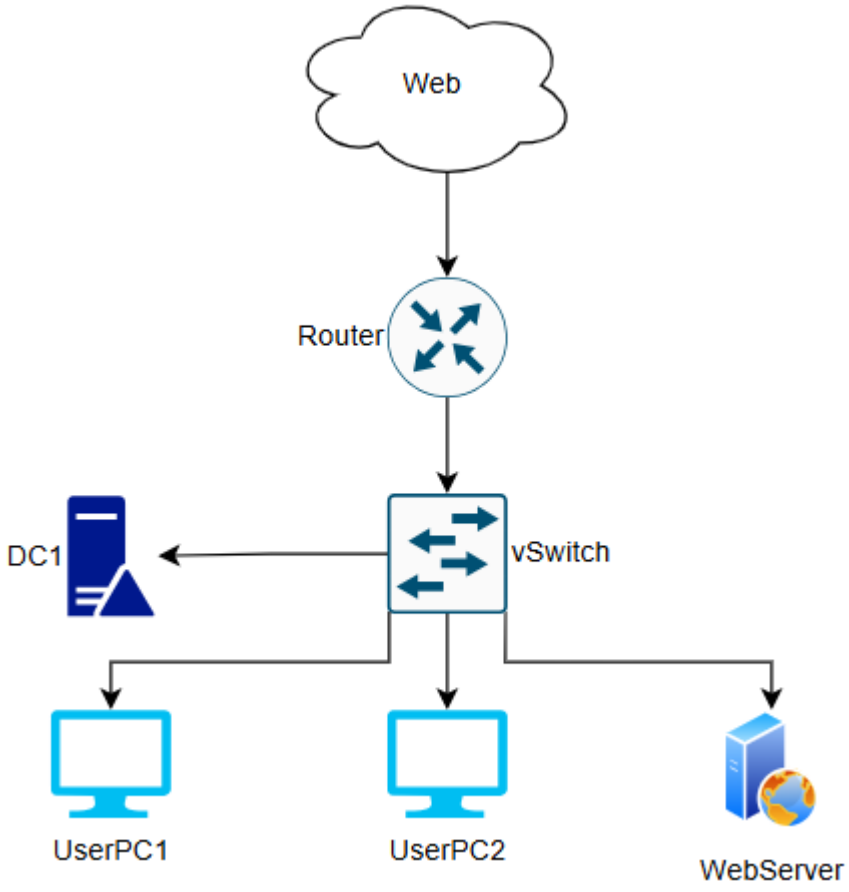

Figure 1 - Test Lab Structure

Evidence and Verification

Implementing a security control is only part of the process. It is also important to demonstrate that it is configured correctly and produces the outcome we expect. The ASD Essential Eight Assessment Process Guide defines four levels of evidence quality and recommends using the highest quality evidence that is reasonably practicable.

At the highest level, a control is tested using a simulated activity to demonstrate that it is both in place and effective. Lower levels of evidence rely progressively more on reviewing configuration, reports or documentation rather than directly demonstrating the control.

Evidence Quality	Testing Process	Notes
Excellent	The control is tested and verified working	This is what we will use during this course, wherever possible
Good	The live configuration is reviewed through the system interface	This shows configuration, but there may be other factors bypassing the configuration
Fair	A copy of the configuration is provided	Screenshots could be from a test system, or old configuration that is no longer valid
Poor	Implementation is described in policy	Policy alone does not demonstrate that the control has been configured or tested

Table 3 - Evidence Quality

For this series, the aim is not simply to show that a setting has been enabled. Where practical, the lab will first demonstrate the behaviour before a control is implemented. The change will then be made and the same activity repeated to demonstrate the difference. This before-and-after approach makes the effect of the control visible and provides stronger evidence that the expected security outcome has actually been achieved.

Next Steps

This guide has introduced the Essential Eight, its maturity model, the Maturity Level One objective used throughout this series, and the test and verification approach that will be applied in the implementation guides.

The next eight guides will address each mitigation strategy individually. They will work through the relevant Maturity Level One requirements, implement them in the test environment, and verify the outcome against ASD's assessment guidance.

The next guide covers **Restrict Administrative Privileges**.